TEXTO APROBADO POR LA COMISIÓN PRIMERA DEL H. SENADO DE LA REPÚBLICA

PROYECTO DE LEY N° 10 DE 2023 SENADO

"POR LA CUAL SE CREA LA AGENCIA NACIONAL DE SEGURIDAD DIGITAL Y SE FIJAN ALGUNAS COMPETENCIAS ESPECÍFICAS"

EL CONGRESO DE COLOMBIA

D E C R E T A:

CAPÍTULO I. CREACIÓN, NATURALEZA JURÍDICA, OBJETO, DOMICILIO Y FUNCIONES

ARTÍCULO 1. OBJETO. La presente ley tiene por objeto establecer la institucionalidad que coordinará, definirá y hará seguimiento a las políticas de seguridad digital o ciberseguridad, implementadas por las entidades públicas y las personas naturales y jurídicas de derecho privado. Establecerá las obligaciones y deberes que tienen los órganos del Estado para determinar los requisitos mínimos para la prevención, resolución y respuesta de incidentes de ciberseguridad.

ARTÍCULO 2. PRINCIPIOS. En el desarrollo, interpretación y aplicación de la presente Ley, además de los principios constitucionales, se aplicarán los que a continuación se prevén:

Principio de Coordinación: Las actuaciones que se realicen en materia de seguridad digital deberán integrar de manera coordinada a las múltiples partes interesadas, para garantizar la armonía en el ejercicio de sus funciones y el logro del objeto de la presente ley.

Principio de Confidencialidad: Todas las personas y organizaciones que intervengan en materia de seguridad digital que tengan acceso a información que no tenga la naturaleza de información pública están obligadas a garantizar la reserva de esta, según corresponda y a través de mecanismos idóneos, inclusive después de finalizada su relación con alguna de las labores que comprende la gestión del riesgo.

Principio de Cooperación: En el marco de las relaciones nacionales e internacionales en materia de seguridad digital, aunarán esfuerzos para el logro de los objetivos de seguridad digital del país.

Principio de Enfoque basado en riesgos: La seguridad de la información y la ciberseguridad deberá estar basada en el enfoque basado en riesgos de forma tal que la definición y aplicación de controles y la toma de decisiones, siempre considere los riesgos como insumo principal.

Principio Perspectiva Interseccional: La Agencia desarrollará sus funciones en consideración de las particularidades de los distintos grupos poblacionales y se regirá con un enfoque de inclusión interseccional en términos de sexo, identidad de género, raza, etnia, capacidad económica, clase social, orientación política y edad; abordando los riesgos e impactos diferenciados de las amenazas y riesgos para que la ciberseguridad responda a necesidades, prioridades y percepciones diferenciadas basadas en las particularidades de cada grupo poblacional.

Principio de Integridad: El Estado desarrollará, a través de las entidades y organismos competentes las acciones necesarias para elevar la confiabilidad y la exactitud de los datos o información de forma que se evite su manipulación, su adulteración y cambios por personas, entidades o procesos no autorizados.

Principio de Neutralidad Tecnológica: El Estado garantizará la libre adopción de tecnologías que permitan fomentar la eficaz gestión de la seguridad de la información y la ciberseguridad, sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos.

Respeto a la privacidad: La seguridad de la información y la ciberseguridad son base del aseguramiento de la privacidad y protección de datos personales, y su gestión deberá incluir medidas formales de protección de la privacidad. La gestión de la seguridad de la

información y la ciberseguridad deberá igualmente, en todo momento, respetar la privacidad de las personas.

Principio de Protección de Datos Personales: Son las acciones administrativas y operativas encaminadas a mantener la privacidad de las personas naturales en un Estado, de acuerdo con lo definido y exigido por el Régimen de Protección de Datos Personales.

Principio de Privacidad: Derecho de los individuos o titulares a su intimidad, de acuerdo con lo consagrado en la Constitución y en el Régimen de Protección de Datos Personales.

ARTÍCULO 3. DEFINICIONES. Para los efectos de la presente Ley, se adoptan las siguientes definiciones:

a. **Agencia:** Es la Agencia Nacional de Seguridad Digital.
b. **Amenazas:** Causa potencial de un incidente no deseado, el cual puede resultar en el daño a un sistema, individuo u organización.
c. **Ciberataque:** Incidente de ciberseguridad en el que una persona o grupo de ellas, conocidas o no, intenta destruir, exponer, alterar, deshabilitar, filtrar, robar, hacer uso o acceder de manera ilícita a un activo de información o de tecnologías de la información, y en el que puedan verse afectados también activos físicos de forma eléctrica o mecánica.
d. **Ciberdefensa**: Capacidad para evitar y responder ante cualquier amenaza o incidente de naturaleza cibernética que impacte la seguridad nacional.
e. **Ciberdiplomacia**: Uso de herramientas diplomáticas para resolver asuntos relativos al ciberespacio.
f. **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios y para almacenar, modificar e intercambiar datos.
g. **Ciberseguridad:** Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que puedan utilizarse. Busca la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios, infraestructuras e información del Estado y de los ciudadanos en el ciberespacio.

h. **Delitos cibernéticos**: Aquellos que afectan la disponibilidad, integridad y confidencialidad de la información y los sistemas digitales. Estos solo pueden cometerse a través y en contra de un sistema informático.
i. **Delitos ciber habilitados**: Aquellos que existían de forma previa a las TICs, pero que, con el desarrollo de éstas, ahora se desarrollan también mediante la modalidad cibernética.
j. **Ecosistema Digital:** Conjunto de infraestructuras y prestaciones (plataformas, dispositivos de acceso) asociadas a la provisión de contenidos y servicios a través de Internet. Este es un sujeto de análisis fundamental para la definición de políticas públicas, en áreas tan diversas como la digitalización de procesos productivos y la protección de la privacidad de los usuarios.
k. **Equipo de respuesta a incidentes de seguridad informática:** Grupo de especialistas multidisciplinarios capacitados para prevenir, detectar, gestionar y responder a incidentes de ciberseguridad, en forma rápida y efectiva, para actuar de acuerdo a procedimientos y políticas predefinidas, que colaboren en resolver la situación presentada.
l. **Incidente:** Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.
m. **Infraestructuras críticas:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.
n. **Protección de Datos Personales:** Son las acciones administrativas y operativas encaminadas a mantener la privacidad de las personas naturales en un Estado, de acuerdo con lo definido y exigido por el Régimen de Protección de Datos Personales.
o. **Privacidad:** Derecho de los individuos o titulares a su intimidad, de acuerdo con lo consagrado en la Constitución y en el Régimen de Protección de Datos Personales.
p. **Riesgo:** La posibilidad de que una amenaza aproveche una vulnerabilidad y cause una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información.
q. **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas.

r. **Sistema de Información:** Medio por el cual dispositivos, redes o plataformas almacenan, procesan o transmiten datos digitales, ya sea a través de redes de comunicaciones electrónicas, dispositivos o cualquier grupo de redes interconectadas o dispositivos o sistemas de información y plataformas relacionadas entre sí.

s. **Vulnerabilidad:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización.

ARTÍCULO 4. CREACIÓN Y NATURALEZA JURÍDICA DE LA AGENCIA. Créase la Agencia Nacional de Seguridad Digital, como una entidad descentralizada del orden nacional, de naturaleza especial que forma parte de la Rama Ejecutiva, con personería jurídica, autonomía administrativa, financiera y patrimonio propio, adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones.

PARÁGRAFO. La Agencia es la máxima autoridad para la formulación y aplicación de las estrategias nacionales y políticas públicas en materia de seguridad digital.

5

ARTÍCULO 5. MISIÓN. La Agencia es responsable de: a) liderar y fortalecer la gestión del ecosistema digital, coadyuvar en mantener un modelo de Ciberseguridad y la gestión de seguridad de la Información en las entidades del estado y de las personas naturales y jurídicas de derecho privado; b) articular la identificación de las infraestructuras críticas del país con las autoridades y entidades competentes; c) coordinar y cooperar con la identificación de amenazas, vulnerabilidades, con el propósito de asegurar las plataformas del estado a través de la confidencialidad, integridad y disponibilidad de la información o de los activos empleados para su transmisión, reproducción, procesamiento o almacenamiento, asociados a los sistemas de información de la Entidades o en el ciberespacio para uso de la ciudadanía y del estado colombiano; y d) generar y coordinar programas de concientización para los colombianos acerca de la detección de amenazas cibernéticas y desarrollar líneas de acción para el fortalecimiento de la industria de Seguridad Digital en el país.

ARTÍCULO 6. DOMICILIO. La Agencia tendrá como domicilio principal la ciudad de Bogotá, D. C.

ARTÍCULO 7. OBJETIVOS. La Agencia será un organismo de carácter técnico especializado que tendrá como objeto la planificación, articulación y coordinación de las políticas de gestión de los riesgos de seguridad digital en el país, prevención de amenazas internas o externas contra el ecosistema digital del país, fortalecimiento de la confianza y seguridad de todas las partes interesadas en el ámbito digital.

PARÁGRAFO. La Agencia no tendrá competencias de policía judicial, ni las que le corresponden a los organismos de inteligencia y contrainteligencia del Estado. En el ejercicio de sus funciones esta entidad garantizará el derecho de hábeas data, el derecho a la intimidad, a la privacidad, a la libertad de expresión en entornos digitales y al buen nombre de los ciudadanos. Cualquier información que obtenga, recopile, almacene, use, circule o suprima la Agencia deberá tratarse exclusivamente en el marco de sus competencias legales, y sólo podrá ser usada, entregada o transferida a otros organismos con previa autorización judicial.

6

ARTÍCULO 8. RÉGIMEN JURÍDICO. Los actos unilaterales que realice la Agencia para el desarrollo de sus actividades son actos administrativos y estarán sujetos a las disposiciones del derecho público.

Los contratos que deba celebrar la Agencia se regirán, por regla general, por las normas de contratación pública. Excepcionalmente, respecto de los contratos que se tengan que realizar para el desarrollo del objeto misional de la Agencia, dicha contratación se regirá por el derecho privado, aplicando los principios de la función administrativa y de la gestión fiscal y estarán sometidos al régimen de inhabilidades e incompatibilidades previsto para la contratación estatal. La Agencia, expedirá un manual de contratación en la cual se reglamente lo previsto en este inciso.

ARTÍCULO 9. FUNCIONES DE LA AGENCIA. La Agencia tendrá, entre otras, las siguientes funciones:

1. Coordinación y colaboración:

1.1. Coordinar y gestionar, como punto de contacto único, la respuesta oficial ante ciberataques en la totalidad del territorio nacional y ser el órgano institucional que brinde información a los ciudadanos sobre los ciberataques que tengan impacto en el territorio nacional.

1.2. Coordinar con los actores del ecosistema de seguridad digital, el entendimiento y fortalecimiento de la gestión de los riesgos e incidentes de seguridad digital, ciberseguridad y protección de datos de la información que soportan la operación del Estado.

1.3. Liderar la implementación de políticas tendientes al fortalecimiento del nivel de madurez de seguridad digital en las entidades del Estado y coadyuvar en la implementación de mejores prácticas de seguridad en los sectores económicos y en la ciudadanía.

1.4. Adelantar acuerdos de cooperación internacional en temas relacionados con Seguridad Digital, Seguridad de la Información, Ciberseguridad, y Privacidad, tanto a nivel de protección de la información y las tecnologías de la información asociadas como las tecnologías operacionales propias de las infraestructuras y sectores críticos, teniendo en cuenta las políticas de Gobierno y la normativa vigente, dentro del marco de los tratados internacionales vinculantes para Colombia y del respeto de la facultad del Presidente de la República de dirigir las relaciones internacionales.

1.5. Organizar y coordinar una Comisión Intersectorial de Tecnologías Disruptivas que monitoree el desarrollo y uso de tecnologías relacionadas con la transformación digital disruptiva en sectores esenciales para el Estado y la ciudadanía como el transporte, la salud, los servicios públicos, los servicios financieros, la seguridad nacional, entre otros según la necesidad, y expida lineamientos, estándares e instrucciones tendientes a garantizar la seguridad de dichas tecnologías y a prevenir y mitigar los riesgos que de ellas se derivan.

1.6. Coordinar y colaborar con agencias de seguridad digital y ciberdefensa de otros países, organismos internacionales y del sector privado con el fin de intercambiar información que pueda abordar los desafíos cibernéticos y coordinar con el Ministerio de Relaciones Exteriores, las acciones de ciberdiplomacia que se requieran para dicho fin.

2. Evaluación y mitigación de riesgos:

2.1. Asegurar el ecosistema digital y su gobernanza, de acuerdo con la dirección estratégica del gobierno nacional y establecer los lineamientos y/o políticas en materia de seguridad y gobernanza del ecosistema.

2.2. Contribuir a la protección y defensa del ciberespacio ante actos de penetración, infiltración, espionaje, sabotaje u otras actividades cuando atenten gravemente contra la administración pública y las infraestructuras críticas y proteger a las instituciones de nivel nacional y territorial de la influencia de organizaciones criminales.

2.3. Contribuir a la protección de recursos tecnológicos y económicos de la Nación, cuando su amenaza comprometa el orden público.

2.4. Brindar asesoría y apoyo técnico a las entidades del Estado, al sector privado y a los ciudadanos en seguridad digital y ciberdefensa.

2.5. Dictar protocolos, estándares e instrucciones generales que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información del país, para reducir los riesgos de seguridad digital de las entidades del Estado, de los diferentes sectores económicos y de los ciudadanos.

2.6. Crear y coordinar un observatorio encargado de realizar análisis de amenazas cibernéticas, y colaborar con entidades públicas, sector privado y ciudadanos en el entendimiento de tácticas, técnicas y procedimientos de los delincuentes ante eventuales ciberataques, de recolectar información y de monitorear ataques tanto a nivel nacional e internacional. El observatorio trabajará en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Relaciones Exteriores, el Ministerio de Educación y la Superintendencia de Industria y Comercio. Los análisis y estudios elaborados por el Observatorio se presentarán al Consejo Directivo a través de informes por lo menos una vez al año.

8

3. Educación y prevención:

3.1. Fortalecer las capacidades y competencias en seguridad digital de los servidores públicos, trabajadores oficiales, contratistas, proveedores y demás grupos de interés que accedan a la información del Estado colombiano.

3.2. Ofrecer en coordinación con el Ministerio de Educación Nacional programas de educación y concientización dirigidos a entidades públicas, sector privado y a los ciudadanos sobre investigación entrenamiento de ciberdefensa y gestión de amenazas, riesgos y ciberataques.Promover el desarrollo nacional de una cultura de ciberseguridad.

3.3. Trabajar de manera conjunta con instituciones educativas y de investigación en temas relacionados con seguridad digital y la ciberdefensa, con el fin de impulsar el desarrollo de nuevas tecnologías para mitigar los riesgos de

ciberataques y de promover la innovación en soluciones de seguridad digital y ciberdefensa.

3.4. Representar al Gobierno Nacional en conferencias especializadas y escenarios académicos internacionales y ante organismos multilaterales, en lo relacionado con la protección de la seguridad digital y ciberdefensa de la Nación

3.5. Construir, en coordinación con el Ministerio de Ciencias, Tecnologías e Innovación, una hoja de ruta para fortalecer la investigación y desarrollo tecnológico en ciberseguridad y el asesoramiento en la creación de startups en la materia.

3.6. Fomentar, en conjunto con el Ministerio de Educación Nacional, el estudio de carreras profesionales enfocadas en la ciberseguridad.

4. Planificación:

4.1. Diseñar y publicar el Plan Nacional de Seguridad Digital y Ciberdefensa, el cual contendrá programas,instrucciones, circulares, órdenes de carácter general y técnica; lineamientos y estándares en materia de seguridad digital, de conformidad con recomendaciones y estándares internacionales.

4.2. La planificación y articulación de actividades orientadas a la identificación y caracterización de activos de información, activos relacionados y activos de infraestructuras críticas;

4.3. Planear, desarrollar, mantener y mejorar de forma continua los modelos de Ciberseguridad y gestión de seguridad de la Información para ambientes de tecnologías de la información y de sectores críticos y/o de control industrial operacional.

4.4. Constituir y coordinar el Observatorio de Seguridad Digital y Ciberdefensa, el cual tiene como fin reunir información sobre los ataques cibernéticos presentados a las infraestructuras críticas de la Nación, así como a empresas privadas y entidades del sector público. El Observatorio presentará sus informes mínimo una vez al año y trabajará en coordinación con el Ministerio de Relaciones Exteriores, Ministerio de Defensa Nacional, el Ministerio de Ciencia, Tecnología e Innovación, el Ministerio de Tecnologías de la Información y el Ministerio de Educación Nacional, la Fiscalía General de la Nación y la Dirección Nacional de Inteligencia.

4.5. Establecer que toda persona jurídica o entidad que administre u opere infraestructuras críticas tendrá la obligación de informar a la Agencia, los reportes de incidentes de ciberseguridad e informar respecto del plan de acción que adoptó.

5. De ejecución:

9

5.1. Desarrollar actividades de Seguridad digital bajo sus principios rectores, en cumplimiento del marco legal y objetivo misional, con las autoridades y entidades competentes.

5.2. Promover el fortalecimiento y la consolidación de los equipos de respuesta a incidentes de seguridad informática de sectores que involucren infraestructuras críticas.

5.3. Coadyuvar en el desarrollo, mantenimiento y mejora continua de los modelos de ciberseguridad y gestión de seguridad de la información para: i) entidades del Estado a nivel de tecnologías de la información, y que sirva de base para las personas naturales y jurídicas de derecho privado; y ii) Infraestructura crítica y control industrial u operacional, sea su propiedad estatal, mixta, o privada.

5.4. Desarrollar actividades de protección del ecosistema digital en cooperación con los demás organismos nacionales e internacionales, así como con otras entidades del Estado y personas jurídicas de derecho privado que administren u operen infraestructuras críticas.

5.5. Ordenar el cese de operaciones en el ciberespacio ante un ataque que afecte la soberanía nacional y el ecosistema digital y su economía, en coordinación con el Ministerio de Defensa.

5.6. Promover la creación, el fortalecimiento y la consolidación de los CSIRTS (Equipos de respuesta a incidentes de seguridad informática) de sectores que involucren infraestructuras críticas, entre los que se cuentan, mínimamente de los sectores de salud; energía; transporte y servicios públicos; así como otros que considere pertinentes.

5.7. Crear el Registro Nacional de Incidentes de Ciberseguridad , el cual tendrá el carácter de reservado. En este registro se ingresaran los datos técnicos y antecedentes necesarios para describir la ocurrencia de incidentes de ciberseguridad, con su análisis y estudio. sobre la base de este registro se podrán realizar las respectivas investigaciones por parte de la Agencia, asi como comunicar las alertas al Consejo técnico y elaborar recomendaciones para subsanar dichas brechas.

5.8. Las demás funciones relacionadas con las actividades de Seguridad Digital que le sean asignadas por el Presidente de la República de conformidad con la Constitución y la ley, siempre que se encuentren dentro del objeto señalado y cumplan con la condición de neutralidad de la presente ley.

PARÁGRAFO 1. El Director General y los servidores públicos de la Agencia, desarrollarán y aplicarán los controles necesarios para garantizar que los procesos de planeación, recolección, procesamiento, análisis y difusión de la información se hagan de manera objetiva y en ningún caso se discriminará el ejercicio de sus funciones por razón de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical, social o de derechos humanos, o para promover los intereses de cualquier partido o movimiento político, o afectar los derechos y garantías de los partidos políticos de oposición.

PARÁGRAFO 2. La Agencia desarrollará sus funciones en estricto cumplimiento del derecho de protección de los datos personales, de conformidad con la normativa vigente y las instrucciones que la Superintendencia de Industria y Comercio imparta en la materia.

CAPÍTULO II. DIRECCIÓN Y ADMINISTRACIÓN.

ARTÍCULO 10. ÓRGANOS DE DIRECCIÓN Y ADMINISTRACIÓN. La Dirección y administración de la Agencia, estarán a cargo de un Consejo Directivo y de un Director General, quien tendrá la representación legal de la misma. El Consejo Directivo, actuará como instancia máxima para orientar sus acciones y hacer seguimiento al cumplimiento de sus fines. 11

ARTÍCULO 11. FUNCIONES E INTEGRACIÓN DEL CONSEJO DIRECTIVO. El Consejo Directivo será responsable de liderar la planificación, coordinación, articulación y gestión de los riesgos de seguridad digital y ciberseguridad en el país, incluyendo aquellos asociados a tecnologías operativas de infraestructura crítica y sistemas de control y actuación industrial, y será el soporte institucional y de coordinación para la definición, ejecución, seguimiento y el control de las estrategias, planes y acciones dirigidas a fortalecer la confianza y seguridad de todas las partes interesadas en el ámbito digital y de las infraestructuras críticas.

El Consejo Directivo de la Agencia, estará integrado por cinco miembros, así:

1. Presidente de la República o a quien designe.
2. El Ministro de Defensa o su delegado.

3. El Director del Departamento Nacional de Planeación o su delegado.
4. El Ministro de Tecnologías de la Información y las Comunicaciones o su delegado.
5. El Superintendente de Industria y Comercio o su delegado.

PARÁGRAFO 1: El Consejo Directivo constituirá un Comité Público-Privado de Estrategia que será el encargado de la planeación de estrategias de largo plazo para fortalecer las capacidades en seguridad digital, potenciar el desarrollo de la industria de ciberseguridad en Colombia y promover la educación de profesionales en el área. El Comité Público-Privado realizará recomendaciones al Consejo Directivo tendientes a atender las amenazas y los riesgos identificados en materia de seguridad digital y presentará informes de actualización sobre ataques perpetrados a nivel mundial y las formas de combatirlos mediante el uso de tecnologías de vanguardia y con los más altos estándares éticos.

PARÁGRAFO 2: El Consejo Directivo, podrá crear grupos de trabajo ad hoc que aborden asuntos científicos y técnicos integrado por representantes de otras entidades públicas o privadas, representantes de los equipos de respuesta a incidentes de seguridad informática de Gobierno y sectoriales, representantes de organismos y gremios del sector privado nacional o internacional, y asesores y expertos de la industria, de la academia y de grupos empresariales o de consumidores, que podrá emitir recomendaciones específicas a nivel de sector y de tecnologías a implementar y participar con derecho a voz, pero sin voto en las reuniones del Consejo Directivo.

12

PARÁGRAFO 3: El Consejo Directivo dictará su reglamento de funcionamiento. Las funciones del Consejo Directivo, y las reglas de creación y composición del Comité Público-Privado y de grupos de trabajo ad hoc se establecerán en el reglamento.

PARAGRAFO 4. Los funcionarios miembros del Consejo Directivo serán responsables disciplinariamente por las faltas que cometan en ejercicio de las funciones asignadas en la presente ley. En especial, la referente a la protección y manejo de los datos personales de las personas. En caso de incurrir en faltas en la materia, serán sancionados según el Código Único Disciplinario o la Ley que la derogue o modifique.

ARTÍCULO 12. DIRECTOR GENERAL Y SUS FUNCIONES. La administración de la Agencia, estará a cargo de un Director General, el cual tendrá la calidad de empleado público,

elegido por el Presidente de la República, a partir de terna presentada por el Consejo Directivo, y será el representante legal de la entidad. Deberá cumplir con requisitos de estudios y experiencia mínimos que establecerá el Consejo Directivo.

Son funciones del Director General las siguientes:

1. Dirigir, orientar, coordinar, vigilar y supervisar el desarrollo de las funciones a cargo de la Agencia.
2. Dirigir las actividades administrativas, financieras y presupuestales, y establecer las normas y procedimientos internos necesarios para el funcionamiento y prestación de los servicios de la Agencia.
3. Ejercer la representación de la Agencia y designar apoderados que representen a la Agencia en asuntos judiciales y extrajudiciales, para la defensa de los intereses de la misma.
4. Dirigir y promover la formulación de los planes, programas y proyectos relacionados con el cumplimiento de las funciones de la Agencia.
5. Presentar para aprobación del Consejo Directivo los estados financieros de la entidad.
6. Aprobar la estructuración técnica, legal y financiera de los proyectos a cargo de la Agencia.
7. Aprobar la estrategia de promoción de los proyectos de concesión u otras formas de Asociación Público-Privada.
8. Orientar y dirigir el seguimiento al desarrollo de los contratos de concesión a su cargo y, en caso de incumplimiento de cualquier obligación, adoptar de acuerdo con la ley las acciones necesarias.
9. Ordenar los gastos, expedir los actos y celebrar los convenios y contratos con personas naturales o jurídicas, así como con entidades públicas o privadas, nacionales o extranjeras, necesarios para el cumplimiento del objeto y funciones de la Agencia.
10. Someter a la aprobación del Consejo Directivo el Plan Estratégico Institucional y el Plan Operativo Institucional.
11. Promover la coordinación de la Agencia con las entidades u organismos públicos y privados.
12. Definir las políticas de comunicación de la Agencia y dar las instrucciones para que estas se cumplan de manera integral y coherente.
13. Proponer al Consejo Directivo la distribución, asignación y cobro de la contribución de valorización en los proyectos que lo requieran, de conformidad con la ley, y

distribuir dicha contribución de acuerdo con las normas vigentes y los lineamientos del Consejo Directivo.

14. Convocar a sesiones ordinarias y extraordinarias del Consejo Directivo y de los Consejos Asesores.
15. Presentar al Consejo Directivo el anteproyecto de presupuesto, las modificaciones al presupuesto aprobado y los planes de inversión de la entidad, con arreglo a las disposiciones legales que regulan la materia.
16. Poner a consideración del Gobierno Nacional modificaciones a la estructura y planta de personal de la Agencia.
17. Distribuir los empleos de la planta de personal de acuerdo con la organización interna y las necesidades del servicio.
18. Distribuir entre las diferentes dependencias de la Agencia las funciones y competencias que la ley le otorgue a la entidad, cuando las mismas no estén asignadas expresamente a una de ellas.
19. Crear y organizar con carácter permanente o transitorio comités y grupos internos de trabajo.
20. Dirigir y desarrollar el sistema de control interno de la Agencia, de acuerdo con la normativa vigente.
21. Cumplir y hacer cumplir las decisiones del Consejo Directivo.
22. Ejercer la facultad nominadora, con excepción de los que corresponda a otra autoridad y dirigir la administración del talento humano de la Agencia.
23. Ejercer la función de control interno disciplinario en los términos de la ley.
24. Las demás funciones que le sean asignadas de conformidad con lo establecido en la ley.

14

ARTÍCULO 13. Créese el rol del Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital como un funcionario de libre nombramiento, más no de libre remoción, por un periodo fijo de cuatro años, el cual tendrá como funciones:

a. Ser el responsable de salvaguardar los derechos de los ciudadanos en relación con sus datos personales en materia de Seguridad Digital.
b. Auditar las actividades de la Agencia Nacional de Seguridad Digital (ANSD) para garantizar el respeto a los derechos de los datos personales de los ciudadanos.
c. Emitir recomendaciones y directrices para mejorar las prácticas de protección de datos en el desarrollo de funciones de la Agencia Nacional de Seguridad Digital.

PARÁGRAFO. El Defensor de los Datos Personales de los ciudadanos en materia de Seguridad Digital, será elegido de una terna de candidatos enviada por gremios del sector de tecnología y la protección de datos y designado por el Procurador General de la Nación.

CAPITULO III. RECURSOS Y PATRIMONIO.

ARTÍCULO 14. RECURSOS Y PATRIMONIO. Los recursos y el patrimonio de la Agencia estarán constituidos por:

1. Los recursos del Presupuesto General de la Nación que se le asignen.
2. Los recursos de crédito que contrate el Gobierno Nacional para el cumplimiento del objetivo de la Agencia.
3. Las donaciones públicas o privadas para el desarrollo de los objetivos de la Agencia.
4. Los aportes de cualquier clase provenientes de recursos de Cooperación Internacional para el cumplimiento del objetivo de la Agencia.
5. Los bienes muebles e inmuebles, así como acciones o títulos representativos de capital de sociedades o activos de la Nación, que le transfiera las entidades del sector y demás instituciones públicas
6. Las propiedades y demás activos que adquiera con recursos propios a cualquier título.
7. El valor de la contribución de valorización de los proyectos a su cargo. Los recaudos que provengan de la ejecución de los proyectos de inversión a su cargo.
8. Los ingresos propios y los rendimientos producto de la administración de los mismos.
9. Los recaudos por concepto de servicios de asesoría y los demás que obtenga a cualquier título.

Los demás que reciba en desarrollo de su objeto.

CAPÍTULO IV. IMPLEMENTACIÓN DE PROTOCOLOS, ESTÁNDARES E INSTRUCCIONES GENERALES Y SANCIONES.

ARTÍCULO 15. Las entidades del Estado y las personas jurídicas de derecho privado deberán implementar dentro de cada organización los protocolos, estándares e instrucciones generales relacionados con seguridad digital que definirá la Agencia de conformidad con las funciones establecidas en el artículo 6 de la presente ley, dentro los 6 meses siguientes a la expedición de la presente Ley

PARÁGRAFO. La Agencia verificará la implementación de los protocolos, estándares e instrucciones generales que expida. En caso de incumplimiento, la Agencia podrá adelantar un proceso administrativo sancionatorio de conformidad con la normativa vigente.

ARTÍCULO 16. Las entidades del Estado y las personas jurídicas de derecho privado domiciliadas en Colombia que administran información cuya divulgación resultaría en la afectación de la soberanía nacional, la estabilidad económica, la seguridad nacional y el derecho al habeas data de los ciudadanos en el ciberespacio deberán informar a la Agencia acerca de posibles riesgos de ciberataques y delitos cibernéticos perpetrados contra sus infraestructuras que supongan riesgos en su información, infraestructura crítica, datos sensibles y sistemas de información. Lo anterior deberá realizarse en un plazo máximo de veinticuatro (24) horas una vez se conozca del hecho, el cual podrá prorrogarse por una sola vez por el mismo tiempo, con el fin de que la Agencia Nacional de Seguridad Digital pueda prestar soporte y ayuda en el momento del ciberataque e iniciar los protocolos necesarios dado el caso y se informe a la opinión pública cuando los hechos efectivamente supongan riesgos de pérdida de información, o impactos de seguridad a infraestructura crítica, datos sensibles, y/o sistemas de información.

Asimismo, las entidades del Estado y las personas jurídicas de derecho privado deberán informar a la Agencia los eventos de materialización de dichas amenazas perpetrados contra sus infraestructuras, en los términos que defina la reglamentación que para el efecto expida la Agencia.

En caso de que las personas jurídicas de derecho privado que administren u operen infraestructuras críticas, no informen de los riesgos o eventos en el tiempo establecido por

la Agencia, se les podrá imponer las siguientes sanciones, a través del desarrollo del proceso administrativo sancionatorio:

1. Multa de hasta doscientos (200) salarios mínimos mensuales legales vigentes. La autoridad competente tendrá en cuenta la capacidad patrimonial para la imposición de la multa.

2. Inhabilidad para contratar con entidades del Estado por un máximo de cinco (05) años, dependiendo del impacto del incidente.

3. Inclusión en la lista que la Agencia conformará de personas jurídicas de derecho privado que no cumplen con buenas prácticas de seguridad digital.

4. Prohibición de recibir cualquier tipo de apoyo, incentivo o subsidio del Gobierno, en un plazo hasta de cinco (05) años, dependiendo del impacto del incidente.

Para los representantes de las entidades del Estado que no realicen los reportes de riesgos, amenazas y eventos de materialización aplicarán las sanciones de acuerdo con lo dispuesto en la Ley 2094 de 2021 y la Ley 610 de 2000 y las normas que las adicionen, modifiquen o sustituyan, por omisión en el cumplimiento de los deberes propios del cargo o función.

CAPÍTULO VI. DISPOSICIONES FINALES.

ARTÍCULO 17. ADOPCIÓN DE LA ESTRUCTURA Y DE LA PLANTA DE PERSONAL DE LA AGENCIA. El Gobierno Nacional, a través del Ministerio de Tecnologías de la Información y las Comunicaciones y en coordinación con el grupo de Transformación Digital del Departamento Administrativo de Presidencia de la República, procederá a adoptar la estructura y la planta de personal de la Agencia, dentro de los seis meses siguientes a partir de la promulgación de la presente ley.

En todo caso, la planta de personal de la Agencia se integrará con cargos ya existentes en el Ministerio de Tecnologías de la Información y Comunicaciones y en el grupo de Transformación digital del Departamento Administrativo de Presidencia de la República. Y

en ningún caso se podrá crear, ni aumentar, ningún gasto burocrático adicional al ya existente.

PARÁGRAFO Hasta tanto se adopte la estructura y la planta de personal de la Agencia, el Ministerio de Tecnologías de la Información y Comunicaciones, en coordinación con el grupo de Transformación digital del Departamento Administrativo de Presidencia de la República cumplirán las funciones señaladas para dicho organismo en la presente ley.

ARTÍCULO 18. APLICACIÓN, VIGENCIA. La presente Ley rige a partir de la fecha de su sanción y promulgación.

EN LOS ANTERIORES TERMINOS FUE APROBADO EL PROYECTO DE LEY N° 10 DE 2023 SENADO *"POR LA CUAL SE CREA LA AGENCIA NACIONAL DE SEGURIDAD DIGITAL Y SE FIJAN ALGUNAS COMPETENCIAS ESPECÍFICAS"*, COMO CONSTA EN LA SESION DEL DIA 31 DE OCTUBRE DE 2023, ACTA N° 16.

PONENTES COORDINADORES:

DAVID LUNA SANCHEZ
Senador de la República

ALFREDO DELUQUE ZULETA
Senador de la República

Presidente,

S. GERMAN BLANCO ALVAREZ

Secretaria General,

YURY LINETH SIERRA TORRES